

CRTC LICENSED OR APPROVED EXEMPT BDUs

TECHNICAL & SECURITY QUESTIONNAIRE

A. General Information:

1. Please provide complete information:

Legal Entity Name	_____
Entity Type (i.e. corporation, partnership etc.)	_____
Owners (list by % owned)	_____
Name of the service ("operating as")	_____
Proposed Areas/Regions to offer service (Territory)	_____
Technical contact (name & email)	_____
Proposed services to be offered on this platform?	_____
Proposed Service Launch Date	_____
Provide Brief Overview of Business Proposition	_____
Date Questionnaire Completed	_____

Business Model(s)

2. Content usage models desired (check all that apply):

- ☐ TVOD (Transactional VOD)
- ☐ PPV (Pay per view)
- ☐ SVOD (Subscription VOD)
- ☐ Pay/subscription
- ☐ AVOD (Advertising supported VOD)
- ☐ EST (Electronic sell-through)
- ☐ Other (describe): _____
- ☐ SD
- ☐ HD
- ☐ 4K

B. System Demonstration

1. Describe the User Interface.

Server Technology

2. Will a CDN be used to distribute content?

☐ Yes ☐ No If "Yes", who is the vendor? _____

3. Attach a detailed System Block Diagram.

Please supply a system block diagram, this should include the following, showing from content ingest, through to encode, encryption, storage, transmission through to client device.

Showing which blocks are co-located and which are not, indicating where the content is encrypted and in the clear.

Please show which links are secured (i.e. VPN, SFTP) and which are in the clear and which are private networks or the internet.

Client Technology

4. Content is delivered to (check all that apply):

- ☐ Set Top Box
- ☐ Game console (specify model(s)) _____
- ☐ PC
- ☐ Mobile (specify model(s)) _____
- ☐ Kiosk based
- ☐ CE device (e.g. TV, BluRay player, etc.) (specify model(s)) _____

5. Please state the operating system (OS) for each device: _____

6. If the client is a Set Top Box, is it based on a PC architecture?

☐ Yes ☐ No

7. If not a PC, who manufactures client device(s)? _____

8. What plans exist for next generation client device development? _____

Video and Audio Technology

9. What video compression codec(s) will be used for content (check all that apply)?

- ☐ MPEG-2
- ☐ MPEG-4/AVC/H.264
- ☐ HEVC/H.265
- ☐ DivX
- ☐ Windows Media/VC-1
- ☐ Other: _____

Content Ingestion

- Describe the security measures in place at the operations center - in particular surveillance system, access control measures, and procedures to manage content.
- What is your content ingestion process? Please include any necessary diagrams and integration points with security (DRM/CAS systems).

Content Encryption

- Which CAS or DRM solution(s) are you using (vendor, product name and version number)?
- Who is implementing the CAS or DRM solution on the devices?
- How is content encrypted? Include algorithm, key size and how often keys are changed.
- What protocol is used to send content encryption keys to the devices?
- How are usage rules uniquely associated with the content and protected against manipulation?
- Is HTML5 video player used?

If yes, please provide the player and DRM for each browser with minimum browser version supported (example: Chrome – JW Player, Widevine, Chrome v.65+).

C. Distribution Platform

Device Summary:

Manufacturer	Device Type	Model Number	Operating System	DRM	Max. Content Resolution	Delivery Type	Network
ex. FOObar, Inc.	ex. Set Top Box	ex. SDF-GH011	ex. Android 2.3	ex. PlayReady 1.2	ex. 480p	ex. Streaming	ex. Internet

- Please provide a table of video & audio resolutions, bitrates, codecs that will be utilized in the service.
- Describe your geo-filtering solution and in the case of Internet distribution the update frequency of the IP look-up table.
- How do you uniquely identify and authenticate devices and/or users? Include exact protocols.
- How do you detect clone devices on the network?

End User Devices

- Is there any tampering resistance (e.g. secure boot, code obfuscation), detection (e.g. jailbreak, root detection) or physical deterrents (e.g. custom case) for the device and/or software?

6. How is the DRM/CAS solution robust against tampering and ensuring device integrity?
7. What is the process to uniquely identify an end user device?
8. How do you securely store keys and other secrets?
9. How are secrets protected when they are being used?
10. For each type of End User Device delivering content, please describe the security measures for end-to-end video delivery including software and hardware video paths and video output control.
11. How do you renew or upgrade the CAS/DRM system?
12. How do you install or upgrade software or firmware?
13. Can the user install third party applications?
14. How do you prevent manipulation of time-based (e.g. rentals) or counter-based (e.g. play counts) licenses?

Video Outputs

15. List all analog video outputs, including resolution and active output protection solution and capability to trigger/control/enforce.
16. List all digital video outputs, including resolution and active output protection solution and capability to trigger/control/enforce.

PVR, Downloads and Transfer to Devices

17. For devices that have the ability to download and/or transfer content to another device:
 - a) How are destination devices uniquely identified?
 - b) How is the content protected?
 - c) How are the usage rules set on the destination devices?
 - d) Is the protection dependent on the content type?
 - e) Is the storage medium uniquely associated with the device?

Usage Rules

18. Do you support a maximum number of concurrent streams across the service? Please explain how this is enforced.
19. Can you limit the number of concurrent streams to a single title? Please explain how this is enforced.
20. What is the total number of permitted devices allowed?
21. Do you track the frequency of device registration/de-registrations? How is this tracked? Can this be limited?
22. If the service allows both streaming and download, how do you enforce concurrent viewing usage rules?

Breach Response

23. How frequently is security examined/reviewed on your delivery system to ensure content does not result in unauthorized distribution/availability?
24. How do you detect security breaches on your system?
25. What measures do you take to address and correct any security breach?
26. What is the communication process to notify Bell Media of any such breaches?
27. What is the process to track resolution for any breach?

Network/Transmission Technology

28. Describe how content is delivered to the central site/NOC:
29. (a) Describe the transmission medium(s) employed for signal delivery (check all that apply):
☐ Twisted-pair copper ☐ Coax ☐ Fiber
- (b) Does the legal entity identified in question A-1 own all the facilities that are used for signal delivery in (a) above?
- Yes ☐
No ☐
- Alternate arrangements (attach detail description) ☐
30. Describe the protocol used to deliver content to the consumer (Network and/or Signal Delivery protocol e.g. Digital or Analogue, ATM, ADSL, IP, cellular etc.): _____

31. Will the proposed IPTV BDU service require a subscriber to also have an internet subscription?
- Yes ☐
No ☐
- If "Yes",
- Will the proposed IPTV BDU service be available through any internet service subscription?

- Will the delivery of the proposed IPTV BDU service have an impact on the subscriber's monthly internet data package or monthly data usage allowance?

Storage

32. Content is:

- ☐ Streamed/linear ☐ Progressively downloaded ☐ Downloaded

If content viewing period is limited, how is expiration date enforced?: _____

If on-demand content is being delivered and the receiving device has recording capability (e.g. DVR/PVR), is recording of such content inhibited?

- ☐ Yes ☐ No

If "No", please explain why: _____

D. Security

1. Digital Rights Management/Conditional Access technology used to protect content:

- | | |
|--|--|
| ☐ Microsoft PlayReady | ☐ FairPlay |
| ☐ Microsoft Mediaroom | ☐ Marlin |
| ☐ OMA 2.0 with CMLA | ☐ DivX |
| ☐ Adobe Flash Access | ☐ Adobe RTMP-E/SWF |
| ☐ CPRM | ☐ AACs |
| ☐ Widevine | ☐ Verimatrix |
| ☐ SecureMedia | ☐ Motorola DigiCipher/MediaCipher |
| ☐ SA/Cisco PoweKEY | ☐ Irdeto |
| ☐ NDS | ☐ Nagra |
| ☐ Conax | ☐ Viaccess |
| ☐ Conklin | ☐ Latens |
| ☐ Secure TV | ☐ Ericsson |
| ☐ Other: _____ | |

2. Is your encryption system smart card based or cardless:

- ☐ Smart Card Based
☐ Cardless

3. Please state version number(s) / version name of DRM/CAS used and mode of operation if applicable:

4. If content is downloaded, is it cryptographically bound to the individual device:

- ☐ Yes ☐ No

If "Yes", please state with what DRM/CAS it is encrypted with: _____

5. Is linear content set to 'copy never' once downloaded onto the device.

- ☐ Yes ☐ No

Mutual Authentication

6. If your service is delivered over an open network, such as the internet, please state how you securely identify the client device, to determine that it is not being spoofed by another device such as a PC.

Regionalization

7. Is this an internet-based service (Are the content servers accessible via any internet connection)?
- ☐ Yes ☐ No
8. How do you geographically limit who is viewing and purchasing the content (two methods required unless closed network):
- ☐ Closed network
 - ☐ IP address database (this generally being the first method)
 - ☐ Verification of credit card billing address
 - ☐ MSISDN
 - ☐ Other: _____

Content Protection

9. Analog video outputs on your system:
- ☐ None ☐ Composite ☐ S-Video
☐ RGB ☐ Component ☐ RF
10. Are all analog video outputs capable of including CGMS-A / WSS?
- ☐ Yes ☐ No
- If "Yes", please confirm you will activate CGMS-A / WSS to the relevant mode:
- "Copyright Asserted, Copying Restricted" (1,1) for On-Demand content:
- ☐ Yes ☐ No
- "Copyright Asserted, Copying Not Restricted" (1,0) for Linear content:
- ☐ Yes ☐ No
11. Uncompressed digital video outputs on your system:
- ☐ None ☐ HDMI ☐ DVI ☐ DisplayPort
12. If uncompressed digital video outputs are present, are they all protected by HDCP?
- ☐ Yes ☐ No
13. Compressed digital video outputs on your system:
- ☐ None ☐ Firewire/1394 ☐ Ethernet ☐ Other _____
14. If compressed digital video outputs are present, are they protected by DTCP?
- ☐ Yes ☐ No

Facility Security

15. Is your facility MPAA approved?

☐ Yes ☐ No

If "Yes", please attach approval certificate.

16. Has this facility received an MPAA Site Audit? When? Who is the MPAA contact?

Also, please describe the security around your facility and your partners including, cctv, security guards, fencing, electronic passes, content server storage, etc.

Please describe your deletion / degaussing procedures for out of license content.

In the case of videotape delivery, is Content encoded in-house or via third-party provider?

If outsourced, please provide details.

Other:

1. Bell Media reserves the right to update and /or change the network security and content requirements and policies as required by our content agreements and to keep up with industry standards.
2. Bell Media reserves the right to audit all solutions prior to launch and once every 12 months thereafter. The audits could be conducted by 3rd party hired by Bell Media.
3. At all times, BDU shall, at its expense, provide, install and maintain in good working order security equipment, systems and procedures that are effective to ensure that the Bell Media content is received only by authorized subscribers, and prevent theft, pirating, unauthorized exhibitions, copying or duplication of the content.
4. All Streaming shall be restricted or Geo-Blocked to the Canadian territories based on the IP address of the individual device/user. BDU shall periodically review the geo-filtering tactics and preform upgrades to the Content Protection System to maintain, at a minimum, industry standard geo-filtering capabilities. Affiliate shall use commercially reasonable best efforts to implement two methods of location verification (i.e. location based services on Apple iOS, certified accounts logins using credit card or billing information).
5. In cases where VOD content in HD is approved for use by BDU on platforms other than set-top-box, pre-approval of a security solution shall be required.
6. Each approved Content Protection System or "CP System" shall be renewable and securely updateable in the event of a Security Breach and allow for integration of new rules and business models. BDU shall implement all software security upgrades available from the Approved CP System vendor promptly, but in no event later than thirty (30) days from such upgrade's release by the vendor.
7. The encryption utilized by BDU's Approved CP System must, at a minimum: (i) use standard time-tested cryptographic protocols and algorithms; (ii) apply encryption to the entirety of the audio and video data with a 128-bit or greater Key strength; (iii) transmit decryption Key(s) protected by encryption to the Authorized Device; (iv) apply a session based cryptographic methodology such that each Key used to protect a piece of content is different for each user authorized to view that content once with all users viewing that piece of content receiving the same decryption Keys(s); and (v) never re-use content encryption Keys.
8. Affiliate shall not to transmit or distribute any Service by means of analog output from any set-top-box or similar or other device in a configuration that is great resolution than 1080 lines, and/or is not interlaced, and or is not a composite signal, or (ii) by means of any digital output from any set-top-box or similar or other device including but not limited to the IEEE 1394 serial bus) or in any digital format.
9. BDU shall not use any resellers or third party transmission agents.
10. BDU will not, and will not allow any third party to white label BDU product or service.

In the event of any conflict between the foregoing and the applicable agreement between BDU and Bell Media, the terms and conditions of the applicable agreement shall govern.

Please confirm your agreement with the foregoing "Other" section:

☐ Yes ☐ No